Healthcare Is Under Cyberattack
Healthcare is one of the top five industries targeted by cyberattacks over the past five years. These disruptions result in lost revenue, negative publicity and patient distrust. Healthcare executives are under intense pressure to protect their organizations from DDoS, insider threats, lost laptops and smart devices, compromised BYOD and other risks that jeopardize the security of highly sensitive patient information.

Enterprises need a comprehensive approach to cyberrisk mitigation. One that goes beyond threat detection and remediation to significantly strengthen incident response and associated data security and recovery strategies.

Cyber Recovery Capabilities Secure Your PHI
Attackers are increasingly targeting backup data—particularly protected health information (PHI)—and most backup systems aren’t designed to recover from cyberattacks. But Unisys Stealth® with Dell EMC Cyber Recovery adds an extra level of protection, so you can maintain HIPAA compliance standards and eliminate any exploitable vulnerabilities in your network.

Unisys Stealth® with Dell EMC PowerProtect Cyber Recovery
Dell EMC recently created a powerful cyber-recovery solution that uses innovative Dell EMC automation, workflow and security analytics tools. This solution employs a backup and recovery data appliance called Dell EMC Data Domain to provide secure and scalable high-speed data backup storage, archiving and data recovery. Unisys Stealth is a software suite that transforms an existing network—both on-premises and in the cloud—into a zero-trust network without requiring changes to existing networks or applications.

STEPS TO TAKE
- Segment your data center based on users. Define and control access to the sensitive information you are entrusted to protect.
- Go undetectable—conceal communication endpoints. Make servers, devices and other communication endpoints undetectable.
- Secure data in motion. AES-256 encryption and patented key management secures data in motion.
- Reduce reliance on physical infrastructure for security. Consolidate physical networks and reduce costs.
- Quickly respond to the needs of your business. Easily update security access privileges through Active Directory.
Stealth principles are simple: trust no user or device (inside or outside the private network) and grant as little access as possible (based upon reliable identification).

Stealth is a “defense-grade” solution that uses identity-based segmentation. Network segments can be defined and managed using an identity management system such as Active Directory or LDAP.

Stealth creates a cryptographic wrapper around the Dell EMC Cyber Recovery vault so it’s virtually invisible to hackers and malware and only allows access to authorized devices.

Why Do Healthcare Organizations Need Unisys Stealth with Dell EMC PowerProtect Cyber Recovery?

Regulations like HIPAA, HITECH, ACA (Affordable Care Act) and Meaningful Use are driving tightened security and controls. Unisys Stealth is designed to securely microsegment data centers and protect data and systems by cloaking strategic assets. Stealth-protected servers or virtual machines are cloaked from other tenants in the cloud and from hackers attempting to infiltrate the cloud.

Why Does It Matter?

$2.2M to $6.9M is the potential cost of failing to secure data

70% of organizations report at least one security incident that negatively impacted operations

72% of enterprises are still immature (or worse) in capabilities involving incident response and recovery


Unisys Stealth with Dell EMC PowerProtect Cyber Recovery

The Unisys Stealth with Dell EMC PowerProtect Cyber Recovery solution protects systems-of-record data in their original form and secures all traffic with (and within) the vault with trusted encrypted access.

Learn More about Unisys Stealth with Dell EMC PowerProtect Cyber Recovery at
